

REMARKS

After the foregoing Amendment, Claims 1-4, 7-8, 10-12, 14-27, and 32-33 are pending in this application. Claims 5-8 have been canceled. Claims 1, 7, and 15 have been amended to more distinctly claim subject matter which the Applicant regards as the invention.

Allowable Subject Matter

Applicant notes with appreciation that claims 10-12, 14, 21-27, and 33 are allowed.

Claim Rejections - 35 U.S.C. § 103

Claims 1-4, 6-8, and 15-18, were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Davies *et al.* (Security for Computer Networks) in view of Arnold (US 6,148,400) and further in view of Puhl *et al.* (US 6,223,291). Claims 5 and 32 were rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Davies, Arnold, and Puhl (same as above) and further in view of Menezes *et al.* (Handbook of Applied Cryptography). The rejections are traversed. Claims 5-6 have been canceled, mooted the rejections as to those claims.

To establish a *prima facie* case for obviousness under 35 USC § 103(a), it must at least be shown that the asserted references, when read alone or in combination, teach all of the elements of the examined claims.

The rejected claims are directed to providing a root key user with the ability to have root keys generated by a root key provider and inserted into the user's message facility by the provider on request or automatically, in a completely secure manner. The root key provider works in conjunction with a secure module supplied by the provider, inserted into the circuitry of

the user's message facility. The module is accessible only by the provider and is completely secure against unauthorized entry, for example, originating at the message facility.

Claim 5 has been canceled, and its features included in claim 1, which now recites that the super-root key of the secure module (such as a secure module of the user's message facility) and the super-root key of the key provider system are the private and public portions, respectively, of an asymmetric private/public-key pair. Claim 15 recites a secure module comprising a super-root key that is a private key of a private/public-key pair. In contrast, Davies discloses symmetric keys, and both Arnold and Puhl disclose storing a public key or certificate containing the public key (presumably a public key of a private/public key pair) at the user's equipment, but not a private key. Likewise, Arnold discloses storing the public key in a secure module, but not a private key. The examiner notes that Menezes explicitly teaches public/private key pairs. However, Menezes also does not disclose or suggest storing a private key in a secure hardware module. Thus, none of the cited references, either alone or in combination, discloses or suggests storing a private key in a secure hardware module, as do claims 1 and 15. Therefore, the 35 U.S.C. § 103(a) rejection of claims 1 and 15 is not supported.

For at least the reasons presented above, independent claims 1 and 15 are deemed allowable over the cited prior art. Claims 2-4, 7-8, and 32 depend from claim 1, and claims 16-18 depend from claim 15. Therefore, without prejudice to their own individual merits, those claims are also allowable for the same reasons.

Claim 19 was rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Davies, Arnold, and Puhl (same as above) and further in view of Easter *et al.* (US 5,559,889). Claim 20 was rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Davies, Arnold, and Puhl (same as above) and further in view of Bergum *et al.* (US 5,249,277). Those claims depend from

claim 15, and it is noted that Easter and Bergum are relied on only for the additional features of claims 19 and 20, respectively. Easter and Bergum do not supplement the other cited prior art with regard to the features of claim 15 not found therein, as discussed hereinbefore. Therefore, for at least the same reasons, claims 19 and 20 are also deemed allowable over the cited prior art.

Based on the arguments presented above, reconsideration and withdrawal of the 35 U.S.C. § 103(a) rejection of claims 1-4, 7-8, 10-12, 14-27, and 32-33 are respectfully requested.

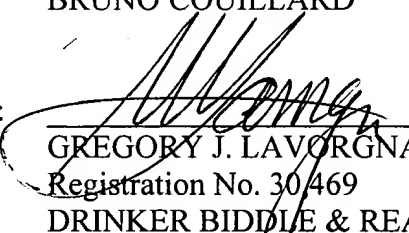
Conclusion

In view of the foregoing amendment and remarks, Applicant respectfully submits that the present application, including claims 1-8, 10-12, 14-27, and 32-33, is in condition for allowance and an early notice of allowance is respectfully requested.

Respectfully submitted,

BRUNO COUILLARD

BY:


GREGORY J. LAVORGNA
Registration No. 30,469
DRINKER BIDDLE & REATH LLP
One Logan Square
18th and Cherry Streets
Philadelphia, PA 19103-6996
Tel: (215) 988-3309
Fax: (215) 988-2757
Attorney for Applicant